

Factorisation en nombres premiers

Exercice 1. $pgcd \times ppcm$

Soient $a, b, c \in \mathbb{N}^*$. Quand a-t-on $pgcd(a, b, c) \times ppcm(a, b, c) = abc$?

Exercice 2. $pgcd \times ppcm$

Soient $a_1, \dots, a_n \in \mathbb{N}^*$ et $b_i = \prod_{j \neq i} a_j$.

Montrer que : $pgcd(a_1, \dots, a_n) \times ppcm(b_1, \dots, b_n) = ppcm(a_1, \dots, a_n) \times pgcd(b_1, \dots, b_n) = \prod a_i$.

Exercice 3. ab est un carré parfait

Soient $a, b \in \mathbb{N}^*$ premiers entre eux tels que ab est un carré parfait. Montrer que a et b sont des carrés parfaits.

Exercice 4. $a^n = b^m$

Soient $a, b \in \mathbb{N}^*$ et m, n premiers entre eux tels que $a^n = b^m$. Montrer qu'il existe $c \in \mathbb{N}^*$ tel que $a = c^m$ et $b = c^n$.

Exercice 5. Valuation 2-adique de $5^{2^n} - 1$

Montrer que la plus grande puissance de 2 divisant $5^{(2^n)} - 1$ est 2^{n+2} .

Exercice 6. $a^r - 1$ premier ?

On suppose que $a^r - 1$ est un nombre premier. Montrez que r est premier, puis que a vaut 2. Réciproque ?

Exercice 7. Nombres de Mersenne

On note $M_n = 2^n - 1$ (n -ème nombre de Mersenne).

- 1) Montrer que : M_n est premier $\Rightarrow n$ est premier.
- 2) Vérifier que M_{11} n'est pas premier.

Exercice 8. $a^n + 1$ est premier

Soient $a, n \in \mathbb{N}$ tels que $a \geq 2$, $n \geq 1$, et $a^n + 1$ est premier. Montrer que n est une puissance de 2.

Exercice 9. Nombre de diviseurs d'un nombre entier

Pour $n \in \mathbb{N}^*$, on note d_n le nombre de diviseurs positifs de n .

- 1) Montrer que si $n = ab$ avec $a \wedge b = 1$, alors $d_n = d_a d_b$.
- 2) Montrer que n est un carré parfait si et seulement si d_n est impair.
- 3) Montrer que : $\prod_{d|n} d = \sqrt{n}^{d_n}$.

Exercice 10. Nombres premiers congrus à 3 modulo 4

Montrer qu'il y a une infinité de nombres premiers p tels que $p \equiv -1 \pmod{4}$.

Exercice 11. Nombres premiers congrus à 1 modulo 4

On rappelle que si p est premier et $n \wedge p = 1$, alors $n^{p-1} \equiv 1 \pmod{p}$.

- 1) Soit $n \in \mathbb{N}$ et $p \geq 3$ un diviseur premier de $n^2 + 1$. Montrer que $p \equiv 1 \pmod{4}$.
- 2) En déduire qu'il y a une infinité de nombres premiers de la forme $4k + 1$.

Exercice 12. Intervalle sans nombres premiers

Trouver 1000 entiers consécutifs non premiers.

Exercice 13. Factorisation de 1000!

Quelle est la plus grande puissance de 6 divisant 1000! ?

Exercice 14. $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$ n'est pas entier

Soit $n \in \mathbb{N}$, $n \geq 2$. Montrer que $x_n = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$ est de la forme : $\frac{p_n}{2q_n}$ avec $p_n, q_n \in \mathbb{N}^*$ et p_n impair.

Exercice 15. *Fonction de Moebius, ENS 2015*

Soit μ définie sur \mathbb{N}^* par $\mu(1) = 1$, $\mu(p_1 \dots p_k) = (-1)^k$ si p_1, \dots, p_k sont des nombres premiers distincts, et $\mu(n) = 0$ si la décomposition de n en facteurs premiers comporte au moins un exposant supérieur ou égal à 2. Pour $n \in \mathbb{N}^*$, on note A_n l'ensemble des entiers $k \in \llbracket 1, n \rrbracket$ premiers à n et $\varphi(n) = \text{card}(A_n)$.

- 1) Simplifier $\sum_{d|n} \mu(d)$ et $\sum_{d|n} \mu(d)/d$.
- 2) Montrer, pour $k \in \mathbb{Z}$: $\sum_{a \in A_n} a^k = \sum_{d|n} \mu(d)(d^k + (2d)^k + \dots + (n)^k)$.
- 3) Déterminer $\lim_{n \rightarrow \infty} \left(\frac{1}{\varphi(n)} \sum_{d|n} \mu(d)(d/n)^k \right)$ lorsque $k \in \llbracket -1, +\infty \rrbracket$.
- 4) Soit $f : [0, 1] \rightarrow \mathbb{R}$ continue. Montrer que $\frac{1}{\varphi(n)} \sum_{a \in A_n} f(a/n) \xrightarrow[n \rightarrow \infty]{} \int_0^1 f$.

solutions

Exercice 1.

a, b, c deux à deux premiers entre eux.

Exercice 2.

Décomposer en facteurs premiers.

Exercice 5.

Récurrence.

Exercice 6.

On suppose a, r entiers supérieurs ou égaux à 2.

$a - 1 \mid a^r - 1$ donc $a = 2$. Si $r = pq$ alors $2^p - 1 \mid 2^r - 1$ donc r est premier.

La réciproque est fautive, $2^{11} - 1 = 23 \times 89$.

Exercice 7.

2) $M_{11} = 23 \times 89$.

Exercice 11.

1) $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$.

Exercice 13.

498.

Exercice 14.

$H_n \Rightarrow H_{2n} \Rightarrow H_{2n+1}$.

Exercice 15.

- 1) Si $n = p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell}$ avec p_1, \dots, p_ℓ premiers distincts et $\alpha_1, \dots, \alpha_\ell \in \mathbb{N}^*$ alors :

$\sum_{d|n} \mu(d) = \sum_{I \subset \{p_1, \dots, p_\ell\}} (-1)^{\text{card}(I)}$, soit la différence entre le nombre de parties de $\{p_1, \dots, p_\ell\}$ de cardinal pair et le nombre de parties de cardinal impair. Cette différence est nulle lorsque $\ell \geq 1$ (regrouper une partie $I \subset \{p_1, \dots, p_{\ell-1}\}$ et $I \cup \{p_\ell\}$) et elle vaut 1 pour $\ell = 0$. Ainsi, $\sum_{d|n} \mu(d) = 0$ pour $n \geq 2$ et $\sum_{d|1} \mu(d) = 1$.

De même, $\sum_{d|n} \mu(d)/d = \sum_{I \subset \{p_1, \dots, p_\ell\}} (-1)^{\text{card}(I)} \prod_{i \in I} (1/p_i) = (1 - 1/p_1) \dots (1 - 1/p_\ell) = \varphi(n)/n$.

- 2) Pour $a \in \llbracket 1, n \rrbracket$, on examine le coefficient de a^k dans chaque membre. A gauche c'est 1 quand $a \wedge n = 1$ et 0 sinon. A droite, en notant $\delta = a \wedge n$, c'est $\sum_{d|\delta} \mu(d)$ soit 0 si $\delta \geq 2$ et 1 si $\delta = 1$.
- 3) En reprenant les calculs de la première question, $\sum_{d|n} \mu(d) d^k = (1 - p_1^k) \dots (1 - p_\ell^k)$ donc

$$\frac{1}{\varphi(n)} \sum_{d|n} \mu(d) (d/n)^k = \frac{(-1)^\ell}{n} \times \frac{p_1 \dots p_\ell}{(p_1 - 1) \dots (p_\ell - 1)} \times \frac{(p_1^k - 1) \dots (p_\ell^k - 1)}{n^k} \xrightarrow{n \rightarrow \infty} 0 \text{ si } k \geq 1.$$

Pour $k = 0$, on a $\frac{1}{\varphi(n)} \sum_{d|n} \mu(d) = 0$ pour tout $n \geq 2$. Pour $k = -1$, on a $\frac{1}{\varphi(n)} \sum_{d|n} \mu(d) (n/d) = 1$ pour tout $n \in \mathbb{N}^*$.

- 4) Si $f(t) = t^k$ avec $k \in \mathbb{N}$, on a

$$\begin{aligned} \frac{1}{\varphi(n)} \sum_{a \in A_n} f(a/n) &= \frac{1}{\varphi(n)} \sum_{d|n} \mu(d) ((d/n)^k + (2d/n)^k + \dots + (n/n)^k) \\ &= \frac{1}{\varphi(n)} \sum_{d|n} \mu(d) (d/n)^k (1^k + \dots + (n/d)^k) \\ &= \frac{1}{\varphi(n)} \sum_{d|n} \mu(d) (d/n)^k B_k(n/d) \end{aligned}$$

où $B_k(\ell) = 1^k + \dots + \ell^k$. Il est bien connu (?) que $B_k(\ell)$ est un polynôme en ℓ de degré $k + 1$ et de terme dominant $\ell^{k+1}/(k+1)$. Donc $(d/n)^k B_k(n/d) = (n/d)/(k+1) + P_k(d/n)$ où P_k est un polynôme. Avec la question précédente,

$$\frac{1}{\varphi(n)} \sum_{d|n} \mu(d) (d/n)^k B_k(n/d) \xrightarrow{n \rightarrow \infty} \frac{1}{k+1} = \int_0^1 f.$$

Le cas des fonctions monôme est réglé. Par linéarité, le cas des fonctions polynomiales l'est aussi. Enfin, pour f continue quelconque, on l'approche en norme $\| \cdot \|_\infty$ par des fonctions polynomiales et on intervertit les limites sans difficulté.